

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-340255

(43) 公開日 平成10年(1998)12月22日

(51) Int.Cl. ⁸	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 E
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00 6 4 0 E
H 0 4 L 9/32		H 0 4 L 9/00 6 7 5 A 6 7 5 B

審査請求 有 請求項の数 4 O L (全 7 頁)

(21) 出願番号 特願平9-151761

(22) 出願日 平成9年(1997)6月10日

(71) 出願人 000164449

九州日本電気ソフトウェア株式会社

福岡市早良区百道浜2丁目4-1 NEC

九州システムセンター

(72) 発明者 後藤 正人

福岡県福岡市早良区百道浜2-4-1 九

州日本電気ソフトウェア株式会社内

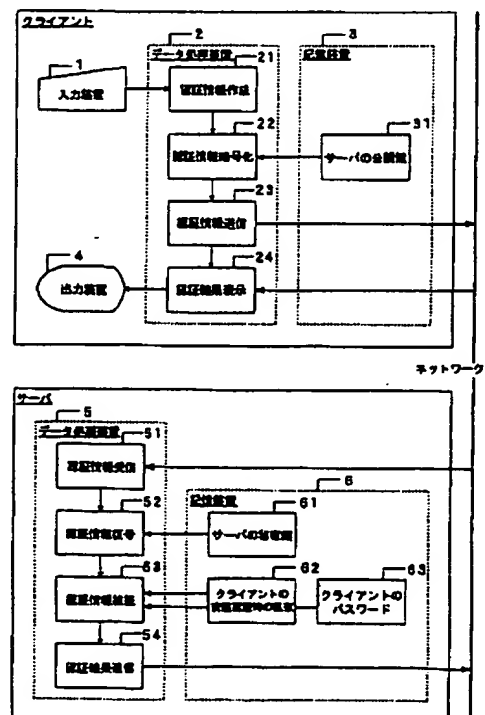
(74) 代理人 弁理士 岩佐 義幸

(54) 【発明の名称】 ネットワーク利用者認証方式

(57) 【要約】

【課題】 ネットワーク利用者認証システムにおける第三者によるクライアントなりすましを防止する。

【解決手段】 クライアントの入力装置1から与えられた利用者識別子、パスワード、有効時間から、認証情報作成21が認証情報有効期限と乱数を作成して、認証情報を作成する。認証情報暗号化22が認証情報をサーバの公開鍵で暗号化し、認証情報送信23が暗号化された認証情報をサーバへ送信する。サーバの認証情報受信51が暗号化された認証情報を受信し、認証情報復号52が暗号化された認証情報をサーバの秘密鍵で復号する。認証情報検証53が認証情報の認証情報有効期限が期限切れでないこと、認証情報の乱数が前回認証時と同じでないことを検証した後、パスワードを検証する。認証結果送信54が認証結果をクライアントに送信し、認証結果表示24が認証結果を出力装置に表示する。



【特許請求の範囲】

【請求項1】ネットワーク上のサーバがクライアントを認証するネットワーク利用者認証方式において、クライアントが、認証情報に認証情報有効期限と乱数を追加する認証情報作成手段を備え、サーバが、認証情報の認証情報有効期限と乱数を検証する認証情報検証手段を備えることを特徴とするネットワーク利用者認証方式。

【請求項2】ネットワーク上のサーバがクライアントを認証するネットワーク利用者認証システムにおいて、クライアントは、キーボード等の入力装置と、サーバの公開鍵をあらかじめ記憶している記憶装置と、ディスプレイ装置等の出力装置と、前記入力装置から与えられた利用者識別子、パスワード、有効時間を基にして認証情報を作成し、作成した認証情報を前記サーバの公開鍵で暗号化し、暗号化された認証情報をサーバへ送信し、サーバから受信した認証結果を前記出力装置に表示するデータ処理装置と、を備え、サーバは、サーバの秘密鍵と、クライアントの前回認証時の乱数と、クライアントのパスワードをあらかじめ記憶している記憶装置と、クライアントから暗号化された認証情報を受信し、暗号化された認証情報を前記サーバの秘密鍵で復号し、認証情報の認証情報有効期限が期限切れでないことと、認証情報の乱数が前記前回認証時の乱数と同じでないことと、前記パスワードを検証し、認証結果をクライアントに通知するデータ処理装置と、を備えることを特徴とするネットワーク利用者認証方式。

【請求項3】クライアントがサーバに送信する認証情報に認証情報有効期限と乱数付加し、サーバがクライアントから受信した認証情報の認証情報有効期限と乱数を検証することを特徴とするネットワーク利用者認証方法。

【請求項4】クライアントの入力された利用者識別子、パスワード、有効時間から、認証情報有効期限と乱数を作成して、認証情報を作成し、作成された認証情報をサーバの公開鍵で暗号化し、暗号化された認証情報をサーバへ送信し、暗号化された認証情報をサーバにて受信し、暗号化された認証情報をサーバの秘密鍵で復号し、認証情報の認証情報有効期限が期限切れでないこと、認証情報の乱数が前回認証時と同じでないことを検証した後、パスワードを検証し、認証結果をクライアントに送信し、認証結果をクライアントの出力装置に表示することを特徴とするネットワーク利用者認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワーク利用者認証方法に関し、特にクライアントがサーバに送信する一方の認証情報のみでサーバがクライアントを認証する機能を有するネットワーク認証方法に関する。

【0002】

【従来の技術】従来、この種のネットワーク利用者認証方法は、ネットワーク上のサーバがクライアントを認証するために用いられている。従来のネットワーク利用者認証方法の一例が、特開平07-325785号公報に記載されている。この公報に記載されたネットワーク利用者認証方法は、認証情報として利用者識別子とパスワードをクライアントからサーバに送信し、サーバは該当する認証情報が存在することを確認して利用者認証を行うシステムにおいて、ネットワーク上の認証情報を保護するために、クライアントは、認証情報をサーバの公開鍵方式の公開鍵で暗号化してサーバへ送信し、サーバは、自分の秘密鍵でそれを復号して認証情報を取り出す。また、クライアントがサーバへ認証情報を送信する前に、サーバがクライアントに乱数をクライアントへ送信し、クライアントが認証情報に乱数を含めてサーバの公開鍵で暗号化してサーバへ送信し、サーバは復号した乱数が先に送信した乱数と同じであることを確認する。

【0003】

【発明が解決しようとする課題】従来の技術において、サーバの公開鍵で暗号化された認証情報を第三者が取得した場合、その者が認証情報の内容を知ることが不可能であるが、クライアントになりすましてその認証情報をサーバへ送信して認証を得ることは可能である。それは、認証情報の内容が毎回同じであるためである。

【0004】このような問題点を解決するために、あらかじめサーバからクライアントへ乱数を送信し、クライアントが認証情報にその乱数を含めてサーバに送信する方法では、サーバとクライアント間で二方向の通信が必要となる。それは、認証情報の一意性を実現する情報をクライアントがサーバから得ているためである。

【0005】本発明の目的は、クライアントからサーバへ送信する認証情報の再利用が不可能となるネットワーク利用者認証方法を提供することにある。

【0006】また本発明の他の目的は、クライアントからサーバへ送信する認証情報が一方のみでセキュリティを確保できるネットワーク利用者認証方法を提供することにある。

【0007】

【課題を解決するための手段】本発明のネットワーク利用者認証方式は、クライアントからサーバへ送信する認証情報に認証情報有効期限と乱数を追加し、サーバがそれを検証する。より具体的には、ネットワーク上のサーバがクライアントを認証するネットワーク利用者認証方式において、クライアントは、キーボード等の入力装置と、サーバの公開鍵をあらかじめ記憶している記憶装置

と、ディスプレイ装置等の出力装置と、前記入力装置から与えられた利用者識別子、パスワード、有効時間を基にして認証情報を作成し、作成した認証情報を前記サーバの公開鍵で暗号化し、暗号化された認証情報をサーバへ送信し、サーバから受信した認証結果を前記出力装置に表示するデータ処理装置と、を備え、サーバは、サーバの秘密鍵と、クライアントの前回認証時の乱数と、クライアントのパスワードをあらかじめ記憶している記憶装置と、クライアントから暗号化された認証情報を受信し、暗号化された認証情報を前記サーバの秘密鍵で復号し、認証情報の認証情報有効期限が期限切れでないことと、認証情報の乱数が前記前回認証時の乱数と同じでないことと、前記パスワードを検証し、認証結果をクライアントに通知するデータ処理装置と、を備えることを特徴とする。

【0008】

【発明の実施の形態】次に、本発明の実施の形態について図面を参照して詳細に説明する。

【0009】図1は、本発明のネットワーク利用者認証方式の実施の形態を示すブロック図である。図1に示すネットワーク利用者認証方式は、クライアントのキーボード等の入力装置1と、プログラム制御により動作するデータ処理装置2と、情報を記憶する記憶装置3と、ディスプレイ装置等の出力装置4と、サーバのプログラム制御により動作するデータ処理装置5と、情報を記憶する記憶装置6とを備えている。

【0010】記憶装置3は、サーバの公開鍵31をあらかじめ記憶している。記憶装置6は、サーバの秘密鍵61と、クライアントの前回認証時の乱数62と、クライアントのパスワード63をあらかじめ記憶している。

【0011】データ処理装置2は、認証情報作成21と、認証情報暗号化22と、認証情報送信23と、認証結果表示24とを備えている。認証情報作成21は、入力装置1から与えられた利用者識別子、パスワード、有効時間を基にして認証情報を作成する。認証情報暗号化22は、認証情報をサーバの公開鍵で暗号化する。認証情報送信23は、暗号化された認証情報をサーバへ送信する。認証結果表示24は、サーバからの認証結果を受信し、それを出力装置4に表示する。

【0012】データ処理装置5は、認証情報受信51と、認証情報復号52と、認証情報検証53と、認証結果送信54とを備えている。認証情報受信51は、クライアントから暗号化された認証情報を受信する。認証情報復号52は、暗号化された認証情報をサーバの秘密鍵で復号する。認証情報検証53は、認証情報の有効期限と、乱数の再現性と、パスワードとを検証する。認証結果送信54は、認証結果をクライアントに通知する。

【0013】本発明の実施の形態の特徴は、クライアントからサーバへの一方向の通信で、サーバがクライアントを認証することにある。クライアントの認証情報作成

21が、認証情報として、認証情報の有効期限と、乱数とを作成し、サーバの認証情報検証53が、クライアントの認証条件として、現時刻が認証情報の有効期限を過ぎていないこと、乱数が前回と同じでないことを検証する。

【0014】次に、図1および図2を参照して、本発明の実施の形態の動作について説明する。図2は、本発明の実施の形態の動作を説明するフローチャートである。入力装置1から与えられた利用者識別子、パスワード、有効時間は、認証情報作成21に供給される。認証情報作成21は、現時刻に有効時間を加算して認証情報有効期限を作成し、乱数を生成する（ステップA1、A2）。認証情報暗号化22は、セッション鍵（共通鍵方式の暗号鍵）となる乱数を生成し、認証情報（利用者識別子、パスワード、認証情報有効期限、乱数）を暗号化し、サーバの公開鍵31を用いてセッション鍵を暗号化する（ステップA3、A4、A5）。認証情報送信23は、暗号化された認証情報と暗号化されたセッション鍵をサーバへ送信する（ステップA6）。

【0015】認証情報受信51は、クライアントの暗号化された認証情報と暗号化されたセッション鍵を受信する（ステップB1）。認証情報復号52は、暗号化されたセッション鍵をサーバの秘密鍵61を用いて復号し、暗号化された認証情報をセッション鍵を用いて復号する（ステップB2、B3）。認証情報検証53は、現時刻が認証情報有効期限を過ぎていないこと、クライアントの前回認証時の乱数62を用いて認証情報の乱数が前回と異なること、クライアントのパスワード63を用いて認証情報のパスワードが正しいことを検証する（ステップB4、B5、B6）。

【0016】認証結果送信53は、認証完了あるいは認証失敗をクライアントへ送信する（ステップB7、B8）。認証結果表示24は、出力装置4にサーバから受信した認証結果を表示する（ステップA7）。

【0017】次に、本発明の実施例について詳細に説明する。図3は、本発明の一実施例を示すブロック図である。図3を参照すると、入力装置1より有効時間が認証情報作成21に供給された場合、認証情報作成21は、認証情報として、現時刻に有効時間を加算して、認証情報有効期限を作成し、乱数を生成する。認証情報検証53は、現時刻を取得し、認証情報有効期限を過ぎていないことと、認証情報の乱数がクライアントの前回認証時の乱数62と異なることを検証する。

【0018】たとえば入力装置1より有効時間として10分が認証情報作成21に供給された場合、認証情報作成21は、認証情報として、現時刻（1997年3月25日11時20分）に10分を加算して、認証情報有効期限（1997年3月25日11時30分）を作成し、乱数（6543210987654321）を生成する。認証情報検証53は、現時刻（1997年3月25

日11時25分)を取得し、認証情報有効期限を過ぎないことと、認証情報の乱数(6543210987654321)がクライアントの前回認証時の乱数62(1234567890123456)と異なることを検証する。

【0019】本実施の形態は、クライアントがサーバへ送信する認証情報に有効期限と乱数を付加することで、認証情報の一意性が向上する。たとえば、第三者がネットワーク上でこの認証情報を取得し、クライアントになりすまして、認証情報をサーバへ送信しても、認証情報の有効期限が切れていたり、すでに同じ乱数で認証済みとなっている可能性が高い。また、認証情報の一意性を高めるために、あらかじめサーバからクライアントに乱数を送信しておき、クライアントが認証情報としてそれをサーバに送信する二方向のネットワーク認証方法があるが、本実施の形態は、同レベルの認証が一方方向で実現でき、効率的である。

【0020】

【発明の効果】以上説明したように本発明は、クライアントが認証情報に認証情報有効期限と乱数を付加して設定するため、クライアントからサーバへ送信する認証情報の一意性が高くなるという効果を有する。その結果、その認証情報を用いてクライアントのなりすましが不可能となる。

【0021】また、本発明は、認証情報の一意性を実現するための情報をクライアントのみで設定できるため、クライアントからサーバへ一方方向に送信する認証情報で、認証情報の一意性が実現できるという効果を有す

る。このため、認証のためのクライアントとサーバ間通信が簡単になる。

【図面の簡単な説明】

【図1】本発明のネットワーク利用者認証方式の実施の形態を示すブロック図である。

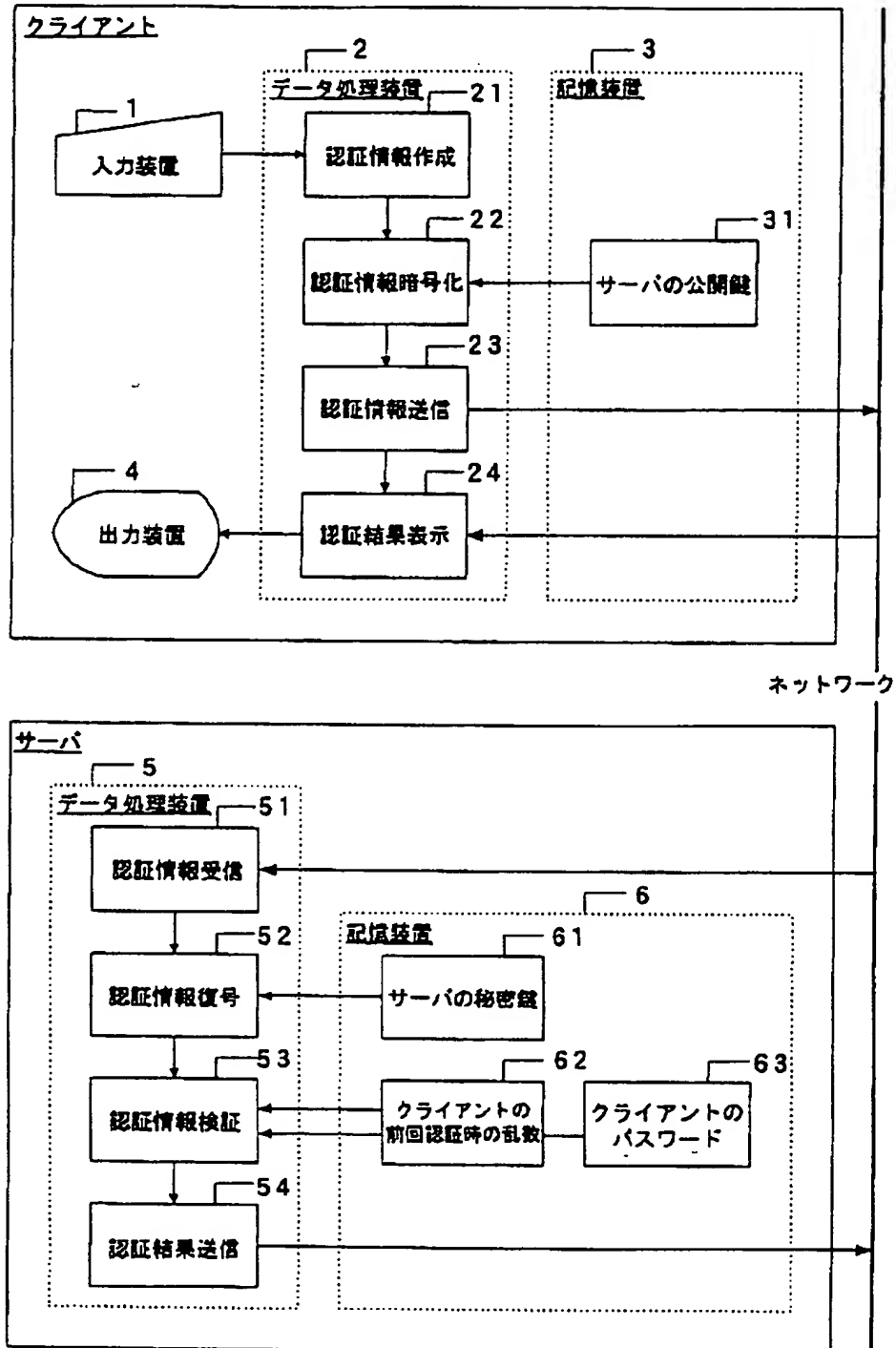
【図2】本発明の実施の形態の動作を説明するフローチャートである。

【図3】本発明の一実施例を示すブロック図である。

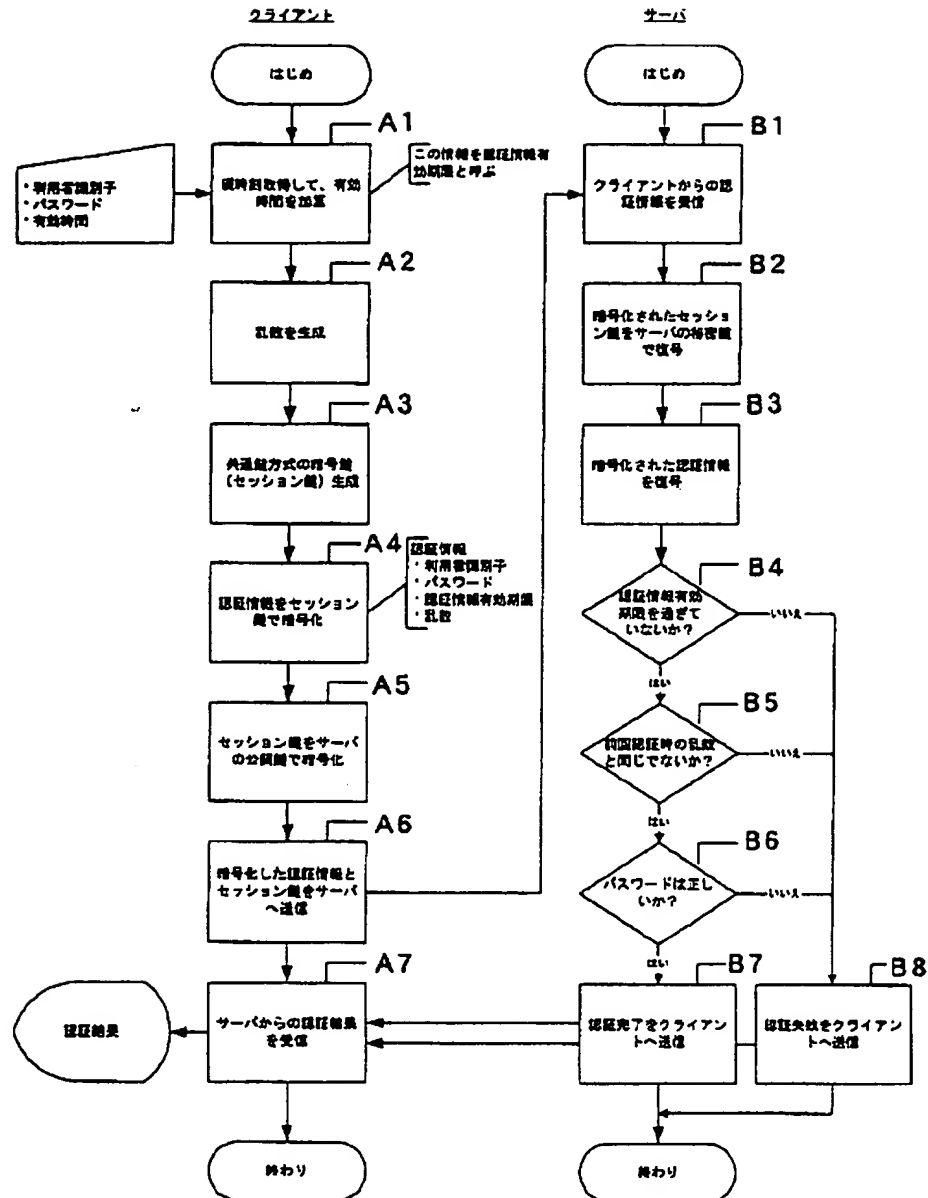
【符号の説明】

- | | |
|----|-----------------|
| 1 | 入力装置 |
| 2 | データ処理装置 |
| 3 | 記憶装置 |
| 4 | 出力装置 |
| 5 | データ処理装置 |
| 6 | 記憶装置 |
| 21 | 認証情報作成 |
| 22 | 認証情報暗号化 |
| 23 | 認証情報送信 |
| 24 | 認証結果表示 |
| 31 | サーバの公開鍵 |
| 51 | 認証情報受信 |
| 52 | 認証情報復号 |
| 53 | 認証情報検証 |
| 54 | 認証結果送信 |
| 61 | サーバの秘密鍵 |
| 62 | クライアントの前回認証時の乱数 |
| 63 | クライアントのパスワード |

【図1】



【図2】



【図3】

